



***Cabinet for Health and Family Services (CHFS)
Information Technology (IT) Policy***



020.303 Security Banner

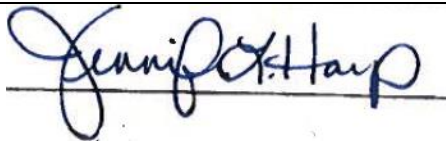

**Version 2.2
March 8, 2018**

020.303 Security Banner	Current Version: 2.2
020.300 Administrative Security	Review Date: 03/08/2018

Revision History

Date	Version	Description	Author
8/2/2002	1.0	Effective Date	CHFS IT Policies Team Charter
3/8/2018	2.2	Revision Date	CHFS OATS Policy Charter Team
3/8/2018	2.2	Review Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
IT Executive, Office of the Secretary (or designee)	3/8/2018	Jennifer Harp	
CHFS Chief Information Security Officer (or designee)	3/8/2018	DENNIS E. LEGER	

020.303 Security Banner	Current Version: 2.2
020.300 Administrative Security	Review Date: 03/08/2018

Table of Contents

020.303 SECURITY BANNER.....	5
1 POLICY OVERVIEW.....	5
1.1 PURPOSE	5
1.2 SCOPE	5
1.3 MANAGEMENT COMMITMENT.....	5
1.4 COORDINATION AMONG ORGANIZATIONAL ENTITIES	5
1.5 COMPLIANCE	5
2 ROLES AND RESPONSIBILITIES	6
2.1 CHIEF INFORMATION SECURITY OFFICER (CISO)	6
2.2 SECURITY/PRIVACY LEAD	6
2.3 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY OFFICER	6
2.4 CHFS STAFF AND CONTRACTOR EMPLOYEES	6
2.5 SYSTEM DATA OWNER AND SYSTEM DATA ADMINISTRATORS.....	7
3 POLICY REQUIREMENTS	7
3.1 GENERAL BANNER INFORMATION.....	7
3.2 WARNING BANNER CRITERIA	7
3.3 IRS WARNING BANNER CRITERIA	7
3.4 BANNER MAINTENANCE	7
3.5 WORKSTATION WARNING BANNER SAMPLE.....	8
4 POLICY MAINTENANCE RESPONSIBILITY	8
5 POLICY EXCEPTIONS	8
6 POLICY REVIEW CYCLE.....	8
7 POLICY REFERENCES	9

020.303 Security Banner	Current Version: 2.2
020.300 Administrative Security	Review Date: 03/08/2018

Policy Definitions

- **Availability:** The reliability and accessibility of data and resources to authorized individuals in a timely manner. The security objective that generates the requirement for protection against intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise cause a denial of service or data.
- **Confidential Data:** Defined by COT standards, is data of which the Commonwealth has a legal obligation not to disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples would include, but are not limited to, data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Confidentiality:** A security principle that works to ensure that information is not disclosed to unauthorized subjects (people, systems, or devices). The security objective that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and while in transit.
- **Integrity:** A security principle that makes sure that information and systems are not modified maliciously or accidentally. The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.
- **Sensitive Data:** Defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include, but are not limited to, information identifiable to an individual (i.e. dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information) and Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)

020.303 Security Banner	Current Version: 2.2
020.300 Administrative Security	Review Date: 03/08/2018

020.303 Security Banner

Category: 020.300 Administrative Security

1 Policy Overview

1.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish an acceptable level of security controls to implement through a Security Banner Policy. This document establishes the agency's Security Banner which helps manage risks and provides guidelines for security best practices regarding security banner notification content.

1.2 Scope

The scope of this policy applies to all internal CHFS employees, consultants, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems. External vendors or other defined groups/organizations providing information security or technology services may work with the CHFS agency(s) to request exceptions to this policy.

1.3 Management Commitment

This policy has been approved by OATS Division Directors, CHFS Chief Technical Officials, and Office of the Secretary IT Executive. Senior Management supports the objective put into place by this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of CHFS property (physical or intellectual) are suspected, CHFS may report such activities to the appropriate authorities.

1.4 Coordination among Organizational Entities

OATS coordinates with other organizations or agencies within the Cabinet with access to applications or systems. All organizational entities that interact with CHFS systems, within or contracted by OATS, are subject to follow requirements outlined within this policy. External vendors, or other defined groups/organizations, providing information security or technology services may work with the CHFS agency(s) when seeking exceptions to this policy.

1.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Applicable agencies additionally follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

020.303 Security Banner	Current Version: 2.2
020.300 Administrative Security	Review Date: 03/08/2018

2 Roles and Responsibilities

2.1 Chief Information Security Officer (CISO)

This position is responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required. This designated position is responsible to adhere to this policy.

2.2 Security/Privacy Lead

Individual(s) designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate personnel. This individual(s) is responsible for providing privacy and security guidance for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff and contractor personnel. This role along with the CHFS OATS Information Security (IS) Team is responsible for the adherence of this policy.

2.3 Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer

An attorney within CHFS Office of Legal Services (OLS) fills the Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer position. This position is responsible for conducting HIPAA mandated risk analysis on information provided by the CISO or CHFS OATS Information Security (IS) Team. The HIPAA Privacy Officer will coordinate with the Information Security Agency Representative, the CISO, or CHFS OATS IS Team, and other CHFS agencies to ensure compliance with HIPAA notification requirements in the event of a breach. This position is responsible for reporting identified HIPAA breaches to Health and Human Services (HHS) Office of Civil Rights (OCR) and keeping records of risk analyses, breach reports, and notifications in accordance with HIPAA rules and regulations.

2.4 CHFS Staff and Contractor Employees

All CHFS staff, contract employees, and other applicable vendor/contract staff must adhere to this policy. All personnel must comply with referenced documents that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

020.303 Security Banner	Current Version: 2.2
020.300 Administrative Security	Review Date: 03/08/2018

2.5 System Data Owner and System Data Administrators

It is the responsibility of these management/lead positions, to work with the application's development team to document components that are not included in the base server build and ensure backup are conducted in line with business needs. This individual(s) will be responsible to work with Enterprise, agency, and application technical and business staff to provide full recovery of all the application functionality and meet federal and state regulations for disaster recovery situations.

3 Policy Requirements

3.1 General Banner Information

CHFS complies with and adheres to the Commonwealth Office of Technology (COT) Enterprise Security Standard Process and Procedures Manual (ESSPPM) as well as governing agencies in regards to context in warning banners.

3.2 Warning Banner Criteria

Screens will include a special security notice. This notice must state: (1) the system may only be accessed by authorized users; (2) users who access the system beyond the warning page represent that they are authorized to do so; (3) unauthorized system usage or abuse is subject to criminal prosecution; and (4) system usage may be monitored and logged. The following subsections detail the access controls and accountability security policies.

3.3 IRS Warning Banner Criteria

Access to IRS Federal Tax Information (FTI), enterprise wide, will contain a warning banner with elements regulated within IRS Publication 1075 Exhibit 8. The following elements must be contained with the warning banner: (1) the system contains U.S. Government information, (2) user actions are monitored and audited, (3) unauthorized use of the system is prohibited, and (4) unauthorized use of the system is subject to criminal and civil sanctions.

Users logging onto CHFS workstations through Virtual Private Network (VPN) are subject to accept/agree to the IRS Publication 1075 Exhibit 8 warning banner criteria as stated above, before access is granted.

3.4 Banner Maintenance

It is the responsibility of COT to install and maintain this security banner on all CHFS equipment.

020.303 Security Banner	Current Version: 2.2
020.300 Administrative Security	Review Date: 03/08/2018

3.5 Workstation Warning Banner Sample

The below text shall be displayed on all CHFS workstations, at logon, to inform staff that such monitoring may occur without warning.



4 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

5 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

6 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

020.303 Security Banner	Current Version: 2.2
020.300 Administrative Security	Review Date: 03/08/2018

7 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- Enterprise IT Procedure: COT-067- Enterprise Security Standard Process and Procedure Manual (ESPPM) Process
- Internal Revenue Services (IRS) Publication 1075
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Social Security Administration (SSA) Security Information